Journal of King Saud University – Science (2011) 23, 311–321

King Saud University

Journal of King Saud University – Science

www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Positive Train Control (PTC) failure modes ☆

Mark Hartong [a,*], Rajni Goel [b,1], Duminda Wijesekera [c,2]

[a] Federal Railroad Administration, 1200 New Jersey Ave SE, Washington, DC 20590, United States
[b] Howard University, Information Systems and Decision Sciences, School of Business, 2600 6th Street, Washington, DC, United States
[c] George Mason University, Department of Computer Science, MS 4A4, 100 University Drive, Fairfax, VA 22030, United States

Received 14 September 2010; accepted 18 December 2010
Available online 25 December 2010

KEYWORDS

Railroad;
Positive Train Control;
Safety;
Risk Analysis;
Failure Modes

Abstract Positive Train Control (PTC) systems can eliminate the consequences of collision or derailment. However, prior to the full-scale deployment of these systems, the Federal Government must conduct a regulatory review and approve the risk analysis of the PTC system performance. The objective of this review is to ensure that the operating environment after installation of the PTC system is at least as safe as the operating environment before the system installation. This paper is intended to provide researchers an understanding of PTC, the reason for its use, the regulatory requirements for the required comparative risk analysis of the PTC system, the critical failure modes that the comparative analysis must address, and future work that would facilitate the risk assessment process.

1. Introduction

Rail operations are ubiquitous throughout the United States. They operate in every state in the US except Hawaii, across a network that exceeds 140,000 miles (BTS, 2003). The 559 freight railroads move over 1.7 trillion ton miles of freight (AAR, 2007). The 22 commuter railroads alone move 1.4 million people daily (APTA, 2007) and the Amtrak intercity passenger service adds over 75,000 more (BTS, 2008).

Failures in existing methods of rail operations can have catastrophic consequences. On September 13, 2008, for example, a safety violation known as a "Signal Passed at Danger (SPAD)" resulted in a collision between a Union Pacific freight train and a METROLINK commuter train, which occurred in Chatsworth, California (Melago, 2008). This collision resulted in the death of 26 people and injuries to 135 more. Another SPAD in Macadona, Texas in June 2004 resulted in 3 deaths and 30 injured when a BNSF freight train and a Union Pacific

☆ The views and opinions expressed herein are that of the authors and do not necessarily state or reflect those of the United States Government, the Department of Transportation, or the Federal Railroad Administration, and shall not be used for advertising or product endorsement.

* Corresponding author. Tel.: +1 202 493 1332; fax: +1 202 493 6478.
E-mail addresses: mark.hartong@dot.gov (M. Hartong), rgoel@howard.edu (R. Goel), dwijesek@gmu.edu (D. Wijesekera).
[1] Tel.: +1 202 806 1649; fax: +1 202 797 6393.
[2] Tel.: +1 703 993 1578; fax: +1 703 993 1638.

Peer review under responsibility of King Saud University.
doi:10.1016/j.jksus.2010.12.003

Production and hosting by Elsevier

freight train collided (NTSB, 2006). A failure of a train crew to correctly line a switch in January 2005 in Graniteville, South Carolina resulted in a collision between two Norfolk Southern freight trains. The collision and subsequent release of chlorine gas caused the death of 9 people, injury to an additional 554, and the evacuation of 5400 for a period of 2 weeks (NTSB, 2005). All of these accidents, and the associated casualties, could have been prevented had a Positive Train Control (PTC) system been installed and operational.

Prior to a US railroad installing and operating a PTC system, the railroad must receive regulatory approval from the Federal Railroad Administration (FRA) of the US Department of Transportation (DOT). As part of that approval process, the PTC system must undergo a comprehensive risk analysis of its failure modes. The regulatory review and approval process is complicated by the fact that there is no formal specification of the failure modes that must be addressed in the risk analysis. Consequently each individual railroad specifies its own failure modes, and in the process may not address the critical issues of regulatory concern, or may address them in such a manner that is not clearly understood by the regulatory agency. In either case, the regulatory review process is extended in order to resolve these misunderstanding, adding both to the cost of the system approval process, as well as delaying the implementation of systems. This paper proposes an open common specification of critical failure modes that must be addressed when preparing the required failure analysis for regulatory review. Not only does it aid in preparing the required failure analysis, but also provides a mechanism for allowing the regulator to more effectively evaluate the risks associated with different proposed PTC system implementations.

This paper proceeds as follows. In Section 2, we will discuss current methods of rail operations, and their limitations, to establish a context for the development of PTC systems. Section 3 will discuss PTC systems, their functionality, and how it can augment or replace existing methods of operation. Section 4 will discuss the regulatory framework in which PTC systems are installed. Section 5 discusses related work as well as the proposed general failure mode model associated with PTC, which can adversely affect system safety in terms of Functional Fault Trees (FFT). Finally, Section 6 summarizes the preceding chapters and outlines future work we believe necessary to relate an FFT to the more natural language Use and Misuse Case descriptions of system behavior and failure modes.

2. Existing methods of operations and limitations

Existing methods of operations for the control of trains can be classified into four basic categories:

- verbal authority,
- mandatory directives,
- signal indications, and
- signal indications supplemented by cab signals, automatic train control, or automatic train stop systems.

When using verbal authority and mandatory directives, the aspects of wayside signals along the railroad do not control train operations. Instead, train operations are controlled by orders from the Train Dispatcher, who takes responsibility for knowing what trains are located where, and ensures that no two trains are issued authority to occupy the same location of track at the same time. The Dispatcher usually issues orders, mandatory directives, speed restrictions, as well as the location of any wayside work crew via two-way radio to the locomotive crew. The train crew are responsible for ensuring that they obey these orders, speed restrictions, and advisories. This is the traditional means of controlling operations in the United States, and roughly 40% of all tracks in the United States are controlled in this manner.

Train operations under signal indications constitute the remainder of the train control operations in the US. Track circuit based signal systems were first installed in the US in 1872, and by 1927 they were centrally controlled in the first "Centralized Traffic Control (CTC)" system and have remained basically unchanged since the 1930s. In CTC, authority for train movements is provided by signal indications. The train dispatcher at the control center determines train routes and priorities, and then remotely operates switches and signals to direct the movement of trains. Some CTC systems have been enhanced to provide direct indications of wayside signal aspects to the locomotive engineer inside the locomotive cab. Signal aspect is the appearance of the signal, as opposed to a signal indication, which is the information conveyed by the appearance of the signal. Further refinements called "Automatic Train Stop (ATS)" or "Automatic Train Control (ATC)" automatically cause the train to stop or reduce speed where an engineer fails to acknowledge a wayside signal.

Cab signals simply relay the external signal indications to a visual display inside the cab of the locomotive, making it easier for the crew to note the signal aspect and the associated order it conveys. Unless operated with ATS or ATC, the cab signal systems do not provide speed or authority enforcement. This approach has several significant technical limitations. First, the location of trains can only be determined by the resolution of a track circuit. If any part of a track circuit is occupied, that entire track circuit must be assumed as occupied. The track circuit's length can be made shorter, but adding additional track circuits requires additional wayside hardware. This imposes additional costs, causing a practical (and economical) limit to the number of track circuits that a railroad can install. Second, the information that can be provided to a train through a rail-based system is limited to a small number of wayside signal aspects or speed data.

In addition, the underlying signal systems to provide the required indications for cab, ATS, or ATC to operate are capital intensive. In 2003, the Class 1 railroads alone spent over $490 million in operation, administration, and maintenance of all types of communications and signaling systems with another $153 million in deprecation of the existing plant on approximately 65,000 miles of track (HR, 2003; STB, 2003). Consequently the deployment of these technologies is limited to those areas where rail throughput needs to be maximized. Less than 5% of route-miles in the US have systems in place, where signal indications are shown in the locomotive cab, on-board enforcement of the signal indications, or both (BTS, 2003).

At best, these traditional methods of train control provide for reactive enforcement of unauthorized train movements after a movement violation has occurred. The inability of cab signals, ATS, and ATC to effectively incorporate collision and accident avoidance measures with the current methods of operations has been the primary motivation for the US

National Transportation Safety Board (NTSB) to ask for PTC (NTSB, 2007).

3. Positive Train Control

PTC does not refer to a particular technology, but any number of possible technologies that provide certain functional behaviors (FRA, 1999a). The common functional requirements, known as PTC Level 1, are:

- prevention of train-to-train collisions, referred to as positive train separation,
- enforcement of speed restrictions (including civil engineering restrictions and temporary slow orders), and
- protection of roadway workers and their equipment operating under specific authorities

PTC Level 1 can be augmented with additional functionality. The additional functionality added is referred to as PTC Levels 2, 3, or 4. Each level is cumulative as shown in Table 1.

PTC systems that provide various functionalities are complex systems in nature and are made up of widely distributed physical, but closely coupled, functional sub-systems. All PTC systems are derivations of a single basic functional architecture, with specific enhancements and modifications to both functions and modes of operations to support the unique requirements and operational needs of the individual procuring railroads. The basic characteristics of a PTC system (FRA, 1999b) are:

- high precision determination of train location independent of track circuits,
- continuous train-to-wayside and wayside-to-train high bandwidth RF data communications network to permit the transfer of control and status information and,
- wayside and train borne processors to process received train status and control data and provide continuous train control as required.

PTC offers significant operational advantages, such as more effective utilization of the track wayside infrastructure, improved reliability and reductions in maintenance costs through a significant reduction in the amount of wayside equipment, and the extension of signal operations in non-signalized territory.

The three major functional sub-systems of a PTC system (Hartong et al., 2006a) are the wayside subsystem, the mobile onboard, and the dispatch/control subsystem. These sub-systems communicate with each other over a variety of communication links. The wayside subsystem consists of elements, such as highway grade crossing signals, switches and interlocks or maintenance workers. The mobile subsystem consists of locomotives or others on rail equipment, with their onboard computer and location systems. The dispatch/control unit is the central office that runs the railroad. Each functional subsystem is implemented using various databases, data communication systems, and information processing equipment.

4. Regulatory framework

The regulatory framework governing PTC is complex, and varies depending on whether the PTC installation is deemed a mandatory or voluntary installation by the FRA. Two different, but complementary, sets of regulations exist for each type of installation. Both consist of amendments by the Federal Railroad Administration (FRA) of the US Department of Transportation (DOT) to the ''Rules, Standards and Instructions (RS&I) (GPO, 2009a) for railroad signal and train control systems. PTC installations that are not mandated for installation are governed by 49 CFR 236 Subpart H. These regulations became effective since June 6, 2005 and are known as the ''Standards for Development and Use of Processor-Based Signal and Train Control Systems'' (GPO, 2009b).

Table 1 Positive train control functionality.

PTC Level	Functionality
1	Prevent train to train collision Enforce speed restrictions· Protect roadway workers
2	PTC Level 1 + digital transmission of authorities and train information
3	PTC Level 2 + wayside monitoring of the status of all switch, signal, and protective devices in traffic control territory
4	PTC Level 3 + wayside monitoring of all mainline switches, signals, and protective devices

Prior to the development of the Subpart H regulations, FRA and the rail industry had recognized that advances in technology in signal and train control systems had overtaken the existing prescriptive signal and train control regulations, and that changes were needed. The advanced technologies coming into use had not been foreseen when the original RS&I had been developed, and consequently these new technologies were being regulated on a case-by-case basis. This caused confusion as to the correct regulatory requirements for the various systems.

The Subpart H regulations eliminate this confusion. They specify an implementation-independent method of promoting the safe operation of trains on railroads that use processor-based signal and train control equipment. These regulations are a performance-based standard with only two simple criteria: First, the new system must be at least as safe as what it replaces. Second, the implementer is responsible for demonstrating the safety claims of the new system. Thus any safety analysis provided must demonstrate this.

The Subpart H regulations are technology neutral, so the railroad is free to pick the implementation technology best suited to their requirements. Since the regulations are performance and risk-based, the railroads and their vendors may customize a technology solution to best fit their individual business cases. In short, this framework opens the potential for increased innovations by removing prescriptive design and technological limitations. These are reflected in the implementations of the basic architectural and functional requirements.

In addition to classification by functionality, PTC systems are also classified by the extent that they are used to augment the exiting methods of railroad operations. Since the approval criteria are based on the demonstrating that the replacement

system is at least as safe as the old system, it is necessary to understand if the PTC system is overlaying or replacing the currently installed system. Full PTC systems completely change or replace existing method of operations. Overlay PTC systems act strictly as a backup to existing method of operations where the existing method of operations remains unchanged. This classification scheme also provides an example of the flexibility for both regulators and regulated entities with respect to enforcement and compliance issues.

The intent of Subpart H regulations also adopts a more pragmatic approach to evaluating risk. Absolute perfection is unrealistic and unobtainable. Even if it were technically feasible to determine all failure modes, the economics of engineering such a system would preclude its deployment. Failure to deploy a system, in turn, may result in a decrease, or loss of safety. Instead the regulation requires the presentation of a valid and demonstrable argument that a system is adequately safe for a given application and operational environment over the lifetime of the system. This means that the risks of product operation have been analyzed, assessed, and mitigated where necessary and a mechanism has been created to ensure that the risk mitigation controls are effective. The only limitation of the regulation is that compliance is voluntary. While the regulations provide requirements that a PTC system must meet if it is installed, it did not require the installation of PTC systems. Although the major railroads were deploying PTC systems, the extremely high cost of doing so relative to the accrued safety benefits resulted in very limited deployment.

As an outgrowth of the head end collision at Chatsworth, California during September 2008, the Congress made a public policy decision in October of 2008 that gave FRA authorization to mandate the installation of PTC systems in the Rail Safety Improvement Act of 2008 (RSIA08) (GPO, 2008). This statutory mandate extends the Level 1 functionality of PTC to include prevention of the movement of trains through switches that are left in the wrong position. It also requires that Class 1 railroads, railroads offering intercity passenger service, and commuter railroads install PTC systems on high-risk lines by December 31, 2015. High-risk lines refer to tracks owned by Class 1 railroads, which carry more than 5 million gross tons of freight per year or toxic by inhalation materials, or any track which carries passengers, regardless of the railroad class.

Given this new statutory mandate, and the aggressive time frame required for completion, the FRA made the decision that a slightly more prescriptive regulatory approach than that provided for in Subpart H was appropriate and began the development of a new 49 CFR 236 Subpart I (GPO, 2010). Subpart I maintains the best features of Subpart H, while allowing for greater reuse of information between railroads that is necessary to demonstrate the safety of the PTC systems and supporting two new critical requirements demanded by the Congress. The first is that FRA certifies that mandatory required PTC systems fulfill the statutory requirements. The second is that railroads submit to FRA a risk based prioritized plan for implementing PTC that ensures interoperability with PTC systems installed by other railroads by April 2010. As with Subpart H installations, Subpart I allows railroads to select the technology that best supports their individual business cases, and maintains the technology neutral pragmatic approach that absolute risk elimination is neither practical nor obtainable.

Subpart H and Subpart I share a common requirement for the submission of a risk analysis of the PTC system being implemented. Both also share a common set of failure modes that must be clearly outlined in order to properly complete the risk analysis.

5. PTC system safety

Like traditional signal systems, PTC systems are designed with the goal of fail-safe operation, even when communications are lost. Unlike traditional signal systems, there is leeway allowed regarding the extent that first and second order safety functionalities are required to be directly associated with the term Overlay. First order safety functionalities are mandatory to ensure safe system operation. Their loss would potentially result in unsafe system operations. Second order safety functionalities are those used in conjunction with another function to ensure safe system operation. Loss of a single second order function will not result in an inability to continue with safe system operations, unless coupled with the loss of an additional second order function.

A Signal Passed at Danger (SPAD) is an example of the consequences of the first and second order failure. In all cases, the train crew are required to comply with their operating rules. One of these rules is that the conductor and the engineer ''call the signal'' as a safety check. Both people must call the same signal, else the conductor or engineer is expected to slow and stop the train until the discrepancy is resolved. Failure of a crew to call the signal could be considered as a first order failure, because it could potentially result in unsafe system operations. However, failure to call the signal does not necessarily result in the train exceeding the limits of its authority. A second failure, for example the failure of the crew to apply sufficient brake, is required. Individually these two failures will not necessarily result in an SPAD, but when taken together they result in the occurrence of an unsafe condition.

5.1. Safety cases under Subpart H

In Subpart H the safety case of a PTC system is documented in two separate documents created by the railroads and their vendors, both of which require review and approval by the government. The first, called the Railroad Safety Program Plan (RSPP), spells out how the railroad plans to address the safety and risk analysis, safety verification and validation, human factors, and configuration management. The second is the Product Safety Plan (PSP).

The PSP is the detailed safety analysis for an individual product. It provides a detailed description of the particular product, its concept of operations, the results of the risk analysis done for the product, verification and validation of the product safety, the human factors analysis of the man–machine interface, required user training, maintenance and repair requirements, and security requirements. Approval of the PSP is based on the extent that recognized standards have been used in the product design, the complexity of the product, its deviation from past design practices associated with existing traditional signal and train control systems, the degree of rigor and precision of the safety analysis, the extent of the verification and validation, how identified faults are addressed, and how the risk analysis compares to the previous case.

5.2. Safety cases under Subpart I

The safety case of a PTC system under the proposed Subpart I also requires the submission of two documents and approval by the FRA. The first of these is the PTC Development Plan (PTCDP). Submitted by a single railroad or a consortium of railroads, the PTCDP contains a detailed description of a particular product, its design, and its proposed operating environment. After review and approval of the PTCDP by the FRA, the FRA assigns a Type Approval. The Type Approval is a formal determination by the FRA that the product, if built and operated as described in the PTCDP, will fulfill the statutory requirements. Once issued, any other railroad may elect to implement the system as described in the Type Approval without resubmission of any of the information associated with the PTCDP. If the railroad elects to implement a variant of the system described in the Type Approval, the railroad may submit an abbreviated PTCDP which references the appropriate Type Approval and describes in detail extensions or changes from the type approved system. The second required document is the PTC Safety Plan (PTCSP). The PTCSP is the railroad specific safety analysis of the as-built system implemented in railroads operating environment.

When combined, the information associated with the PTCDP and the PTCSP is equivalent to that presented by a railroad in a PSP submitted under Subpart H. FRA uses the same general criteria used for approval of the PTCDP and PTCSP as used in Subpart H for approval of the PSP. This equivalence is by design – it enables both FRA and the railroads to use the experience gained in formulating and reviewing a PSP under Subpart H to be applied to the formulation and review of filings under Subpart I. Approval of the PTCSP by FRA acts as the system certification required under the RSIA08.

The proposed Subpart I does not require the creation, submission, and approval of a Railroad Safety Program Plan. In crafting Subpart I, FRA promulgates for the railroad the manner in which it is to address the safety and risk analysis, safety verification and validation, human factors, and configuration management based on the type of system (non-vital overlay, vital overlay, standalone, or mixed) and the speed at which rail operations will be conducted. The elimination of the requirement of an RSPP, and the introduction of the type approval, reduce the regulatory burden on the railroad and shorten the system approval process.

5.3. Previous work in the definition of PTC failure modes

To the author's best knowledge, this work is unique in that it is specifically oriented towards specifying taxonomy of PTC system failures. The open literature that discusses PTC failure modes is quite limited. This is not entirely unexpected. The engineering effort associated with failure modes analysis on complex systems, such as PTC is significant and represents a significant cost to the system developer. Open disclosure of the failure mode analysis could allow other suppliers to leverage their engineering effort off the information disclosed, thereby reducing their development costs and gaining a corresponding competitive advantage in the market place. Likewise, in a litigious society such as the US, open voluntary disclosure of failure mode information may place the supplier at risk from expensive litigation by providing the plaintiff information that they try use against supplier. Even US federal regulatory bodies responsible for safety oversight have found it necessary to resort to the threat of formal subpoenas at times to obtain failure mode information.

Recent literature that is available remains oriented primarily towards Automatic Train Control and Protection Systems, and the discussion of system failure modes is secondary to other objectives. Lawson (2007), for example, discusses some failure modes when describing an Automatic Train Control system in use in Sweden. Evans and Verlander (1996) provide some discussion of possible failure in the case of automatic train protection but this is secondary to a methodology for projecting the number of injuries and fatalities in the event of an accident. In Gheorghe et al. (2005), some failure modes are discussed, however, their primary objective of the work is to describe the construct of a possible decision support tool for accident evaluation. Monfaclone et al. (2001) identify some possible train control system failure modes, but for Direct Traffic Control Systems, and in the context of a probabilistic modeling tool called ASCAP. Similar situations exist with Braband (1997), Brabrand and Renpenning (2001), Noffsinger et al. (1999), Jo and Hwang (2007), Yang et al. (2010), Mokkapatia (2004) and Jo et al. (2007). Zhao et al. (2009) discuss failures associated with the communication subsystem of Communications Based Train Control System in the context of demonstrating a safety analysis approach. Chabanon (2005) also discusses some failure modes of CBTC systems, but in the context of commissioning tests of PTC systems. Even Jackson (2005), which specifically addresses CBTC and PTC systems, concentrates on the risk evaluation process as opposed to the identification of the actual failure modes.

5.4. Failure mode model

The safety critical failure modes the PTC system design must address are the same regardless of the regulatory approach it is qualified under. Traditionally, Functional Faults Trees (FFT) have been used in the safety critical design to specify and analyze potential faults in a system's functional architecture, which may result in system failure. Structured FFT Analysis (Vesely et al., 1981) defines event relationships resulting in a failure using Boolean algebra. By simplifying such Boolean algebra expressions, these events can be expressed as combinations of basic faults that result in the system failure so that their removal can result in a system that is devoid of known modes of failure. By associating the estimation of the probabilities of various failure modes the aggregate probability of failure of a system can be determined. A more detailed example of this process for a PTC system can be found in Hartong et al. (2006b). The use of FFT's in this manner is not without precedence. Katsumata et al. (2000) utilize a similar fault Tree Analytical approach, but for an Automatic Train Protection system.

Failures of a PTC system that can result in unsafe train operations can be divided into two basic categories: Train Derailment and Train Collisions, Train Derailment hazards are all failures that result in the train, or any part of the train, leaving the tracks. Train Collision hazards are all failures that result in a train colliding with another object. Both these categories consist of implementation independent, and implementation specific, failures. Specification of implementation specific failures requires knowledge of the

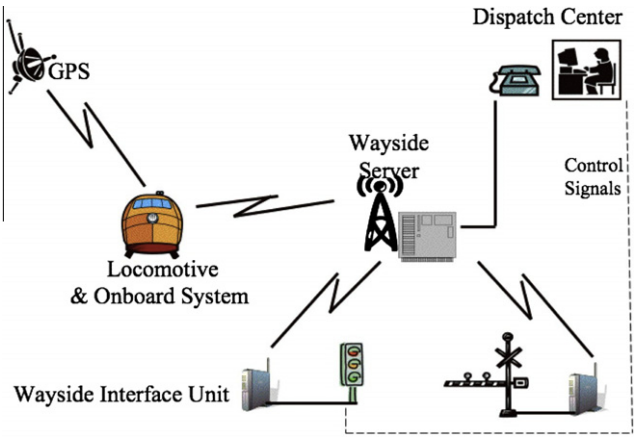

Figure 1 Generic positive train control system architecture.

details of the construction of the PTC system. The details associated with implementation specific failures are usually proprietary intellectual property of the system manufacturer, and are not generally made available to the public. As a consequence, we will only address implementation independent failures (Fig. 1).

5.4.1. Train derailments

Causes of train derailments can be partitioned into four subcategories (Fig. 2). The first of these are infrastructure failures. Infrastructure failures are a consequence of track failures, such as broken rails, excessive increases in the super elevation of the track or changes in track gauge. Because detection and reporting of these types of infrastructure failures are not functional capabilities of PTC Level 1 system (or Level 1 enhanced with switch position monitoring) we will not further develop their underlying causes.

The second category is traversal of a switch incorrectly aligned for the train movement (Fig. 3). Three different conditions can cause this hazard. The first is the movement of the switch after the train has passed the safe stopping distance (SSD) to the switch. The second is that the train actually passes across a misaligned switch. The former is the consequence of an improper command to the switch, the manual movement of the switch, or a failure of the switch controller. The later could be caused by a failure of the switch position indicator to detect the switch position, or a failure of the wayside system to convey the position to the train. The third is the failure of the wayside system to provide the correct aspect to the crew.

Failures to convey the switch position correctly can be attributed to a number of possible system faults. These include generation of a false proceed by the wayside system or generation of a false proceed by the onboard system. False proceeds result from a wayside system display failure that results in the display incorrectly indicating the actual switch position to the crew or a wayside or onboard system failure that conveys an incorrect aspect.

The third category associated with the derailment of a train occurs when a train is moving at a speed in excess of an appropriate speed for the track conditions (Fig. 4). For a train to over speed two conditions must be met. The first is that the train crew are operating the train at a speed greater than that authorized for the track and the PTC system must fail to properly enforce the authorized speed. In order for the train crew to operate the train at a speed greater than authorized, either the train crew are not complying with the railroad operating rules, or the authorized speed provided to the train crew exceeds a safe operating speed for the track conditions.

Providing a speed to the crew greater than the safe operating speed can be the result of the failure of the PTC system to correctly display the operating speed to the crew, providing an incorrect permanent speed restriction to the PTC system, providing an incorrect temporary speed restriction to the PTC

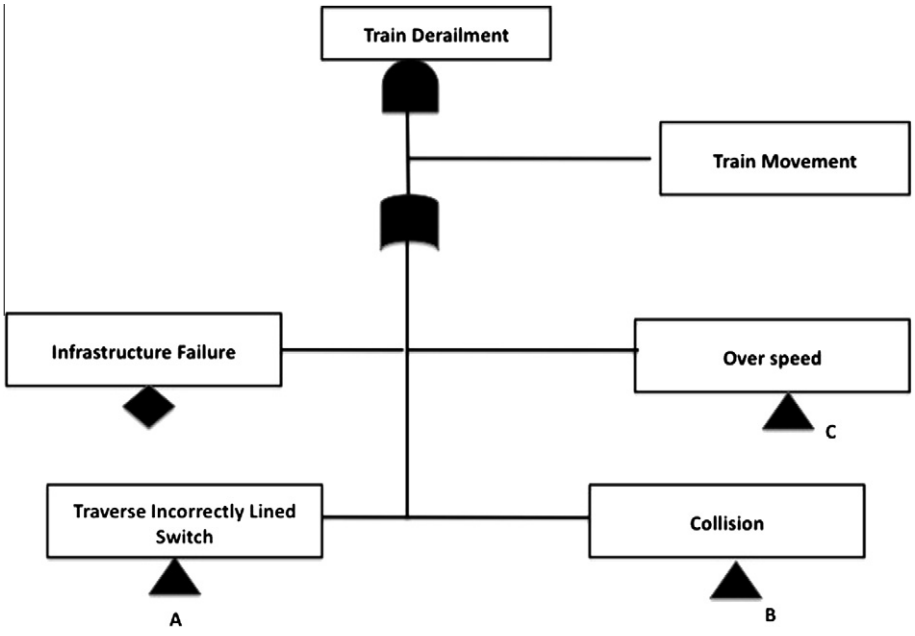

Figure 2 Top level derailment failure modes.

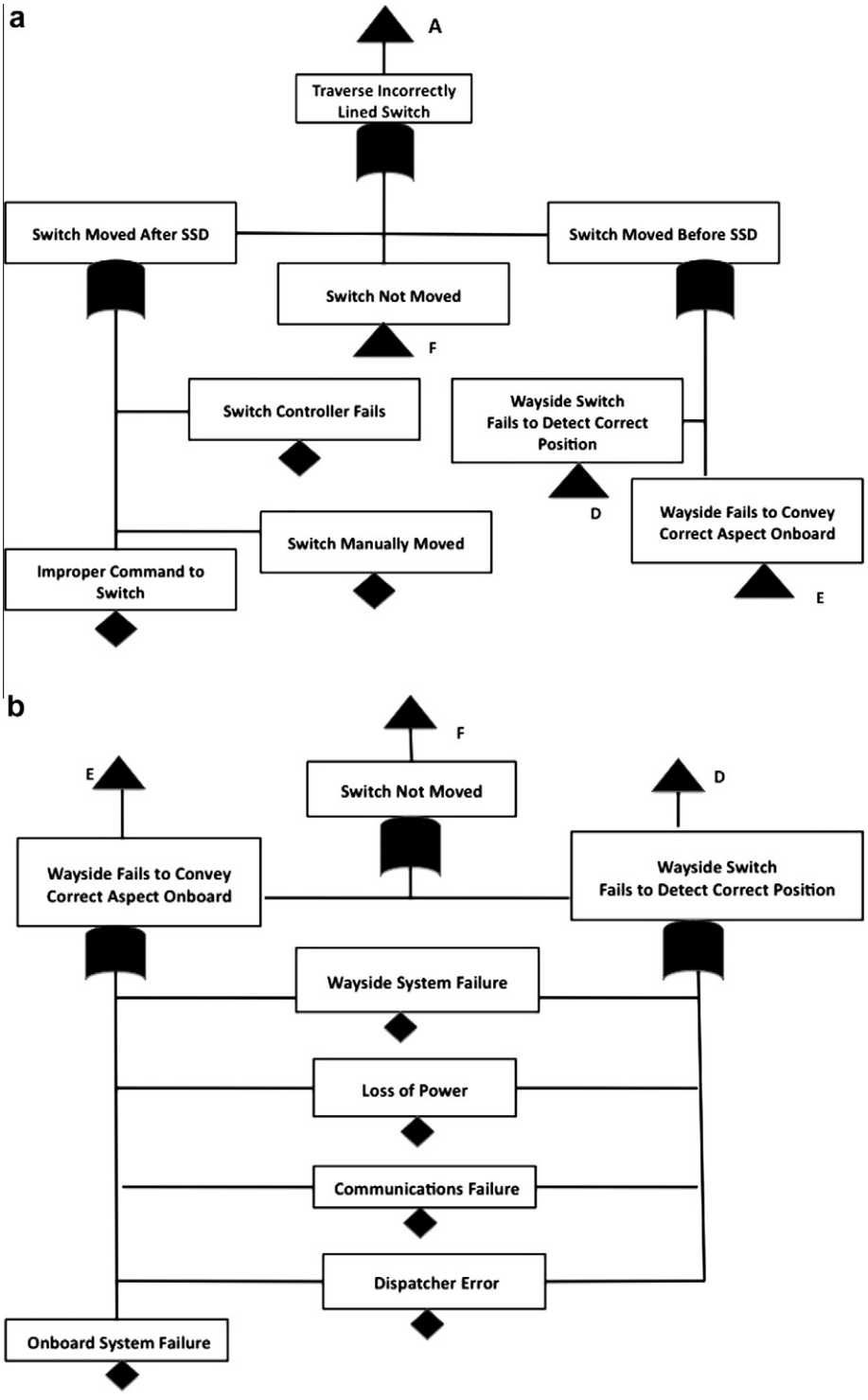

Figure 3 Switch failure modes.

system, or a failure of the wayside system to convey correct speed to the train. Invalid temporary or permanent speed restrictions provided to the PTC system are the result of dispatcher error.

PTC system failures where the PTC system fails to properly enforce the authorized speed are the consequence of a PTC system failure itself, or a failure of the PTC system to provide sufficient braking force to de-accelerate the train. PTC system failures include failure to enforce a permanent speed limit, failure to enforce a temporary speed, or a failure to be able to determine the correct speed limit due to a database error where the correct speed limit cannot be found. Insufficient braking force to de-accelerate the train can be the result of brake system failure or the PTC system braking characteristics being incorrect. Brake systems are not a part of the PTC system, although the PTC system commands when they should be

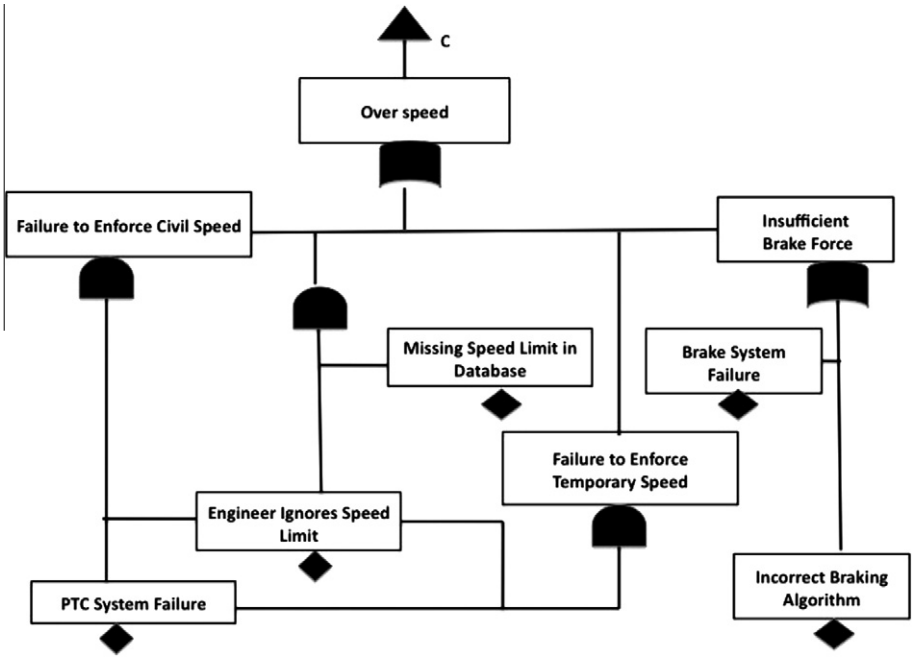

Figure 4 Over speed failure modes.

applied. Since the brake system is not specifically a part of the train control system, but the locomotive control system, further development of this failure mode will be excluded as being more appropriate to a study of the locomotive failures. The other cause of a failure to enforce can be the result of the system having been provided an incorrect braking algorithm.

Failure to properly enforce temporary speed restrictions may also be caused by failure to enter the temporary speed restriction, entry of an incorrect temporary speed restriction, or incorrect removal of a temporary speed restriction. These could be caused by an error on the part of the dispatcher or the crew, or an internal failure on the part of the PTC system resulting in a failure to accept the speed restriction, corruption of the speed restriction, or incorrect removal of a speed restriction.

Both the second, traversal of switch incorrectly aligned for train movements, and the third categories, derailment resulting from speeds in excess of appropriate speed for track conditions, share a common cause, which are not associated with any failure of the PTC subsystem. The act of the crew securing power to the onboard PTC system, maintenance personnel securing power to wayside units, or office personnel securing power to the office system result in the inability for the PTC system to operate. The act of securing power to a PTC system component may be a consequence of an operator error or the actions of a mal-actor. Hence a failure may not only be a safety issue, but a security issue as well.

The fourth subcategory is derailment as a consequence of a collision.

5.4.2. Collisions

Train collisions can be head end to head end between trains on the same track, head end to rear end collisions on the same track, or side collisions between trains on conflicting routes (Fig. 5). Each is the consequence of three different possible events: failures to establish correct routes, failure to enforce routes, or trains over speeding for the track conditions resulting in overrunning limits of authority. The underlying causes for a train over speed have been discussed earlier in conjunction with derailments. The causes of a failure to establish correct routes and failure to enforce correct routes are common regardless if they result in a head end to head end, head end to rear end, or side collisions.

Route selection failures can be attributed to failure of the PTC wayside equipment to generate the correct routing signals, or failure of existing wayside equipment allowing unsafe train movement. Collisions arising from failure of wayside equipment, which allow an unsafe movement, can be the result of the failure of the PTC system to correctly display the route to the crew, the office dispatch system providing an incorrect route to the PTC system, or a failure of the wayside system to convey the correct route to the train. Failures to enforce a correct route can be attributed to failure of the wayside equipment to execute the correct commands to protect against conflicting routes, or failure of the PTC system to enforce commands that prevent conflicting routes.

PTC system failures that prevent enforcement against conflicting results could include failure of the PTC system to receive the correct route from the wayside or office, failure of the PTC system to generate appropriate braking commands to protect received routes, or failure of the braking system to properly implement the braking commands.

Train collisions are not necessarily with other trains. Trains can collide with maintenance personnel conducting track repairs, hay-rail vehicles operating on the track, train collisions at highway grade crossings, collisions with individuals trespassing across the track, collisions with other objects that have fallen onto the tracks, and collisions with end of track protection devices. Collisions with maintenance personal are the result of an unauthorized incursion into the work zone by the train, or maintenance personnel working outside the

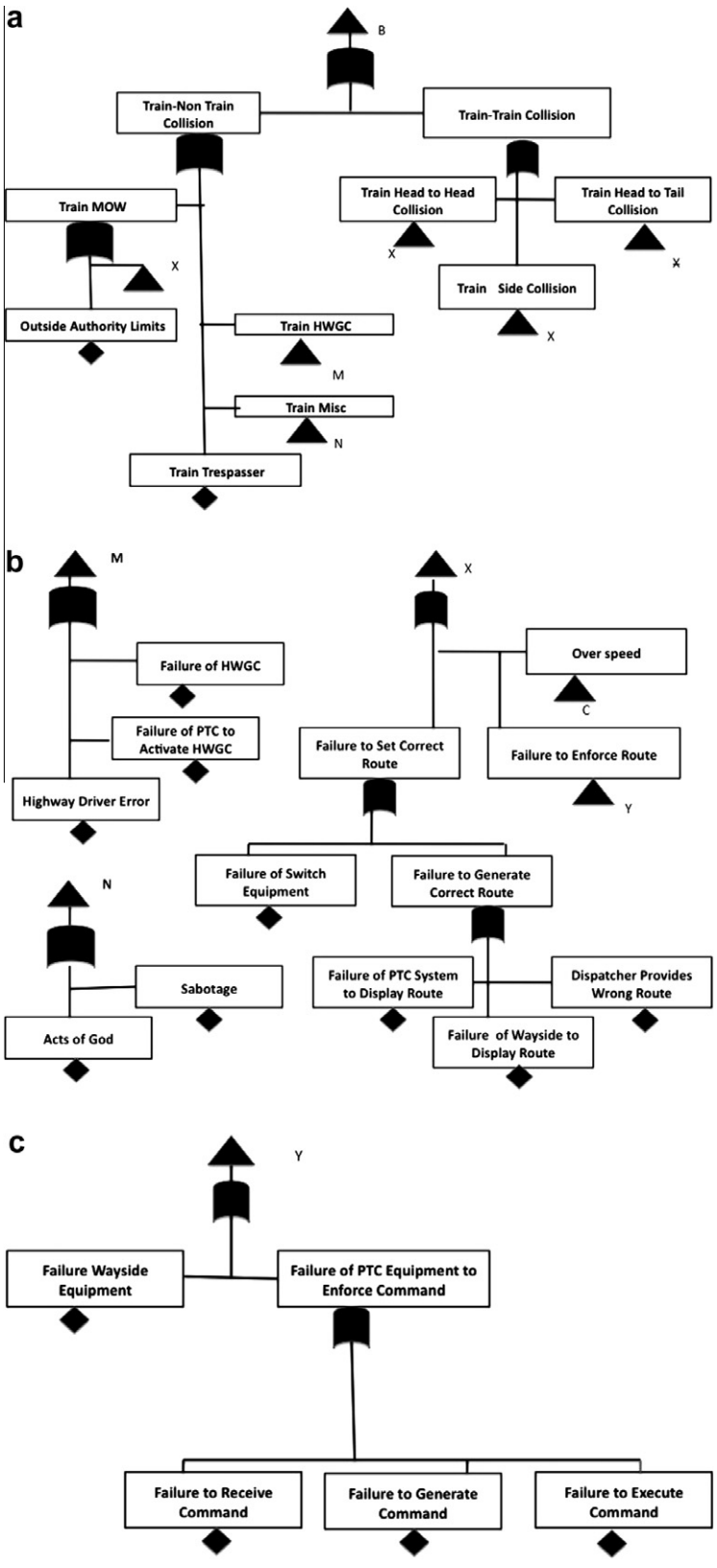

Figure 5 Collision failure modes.

limits of their authority. Causes of unauthorized incursions by the train into the work zone are the same as the causes associated with train-to-train collisions. Maintenance personnel working outside the limits of their authority can be attributed to various human factor issues that are not a result of a PTC system failure and, therefore, are outside the scope of this

paper. Collisions with hay-rail vehicles operating on track can be the result of issues with the PTC system, also similar to those associated with train-to-train collisions, or the hay-rail vehicle operating outside the limits of its authority. Like train collisions with maintenance personnel, operations of the hay-rail vehicle outside the limits of authority can be attributed to various human factors that are outside the scope of this paper.

Collisions with trespassers by a train are not considered PTC preventable accidents. A person trespassing on railroad property onto the tracks is currently not detectable. As a consequence the PTC system is unable to provide either predictive or reactive braking to avoid collision. What causes persons to trespass is not fully understood, and is a subject of active research (FRA, 2007, 2008), and is outside the scope of this paper.

Train collisions at highway grade crossings are attributable to three separate causes, two of which are well understood, and one that is not. The causes that are understood are a consequence of a failure of the PTC system that has the capability to arm the crossing before the train reaches the crossing, or a failure in the operation of the grade crossing. However the third cause, incursion of drivers into a properly operating and activated crossing is not. As with trespassers, the rationale for the driver's actions is a subject of active research, and similarly is outside the scope of this paper.

Collisions with other objects that have fallen onto the tracks are also usually not preventable by PTC systems. Some may be ''Acts of God'', where objects such as trees disturbed by weather or rocks are displaced as a consequence of erosion. Others may be the result of actions by mal-actors placing items on track to induce a collision and a subsequent derailment. In advanced Levels 3 and 4 PTC systems, slide fences that can detect the accidental incursion may be linked into the PTC system and, provided that the PTC system does not otherwise fail, may be able to prevent collisions.

The final category of collisions may be the consequence of a train exceeding the limits of its authority and interacting with end of track protection devices. These include bumpers placed at the absolute physical end of track devices, or derails placed on a track to create a virtual end of track. Causes for collisions of the first type, as well as the second type, are the same as those associated with train-to-train collisions.

6. Summary and future work

The safety of PTC systems in the United States is governed by extensive federal regulations, compliance with which must be demonstrated before a railroad may place any PTC system into revenue service. A critical element of these regulations is the requirement that a railroad perform a detailed quantitative analysis comparing the risks before, and after, the installation of the PTC system. We have described a minimal set of consequences associated with system failure and their implementation independent causal factors that provide system designers a baseline that can be extended with the implementation dependent causal factors, facilitating accomplishment of the required comparative analysis. The use of a common baseline not only enables a more rapid analysis and review of these systems by vendors, railroads, and the government, but also simplifies comparisons of different system.

Extension of the baseline to define common failure modes between differing implementations can further facilitate system comparisons. This work, however, requires access to detailed proprietary system design information from the various PTC system suppliers. It is further complicated by the need to ensure that the analysis results do not disclose the details of any specific vendors proprietary information to their competitors.

Another critical area of research is the derivation of the appropriate FFT from the system specifications. We believe integrating UML Use Cases (OMG, 2005) with Misuse Cases (Opdahl and Sindre, 2001; Alexander, 2002) that are commonly used to capture functional requirements with FFT specification and analysis provides an integrated method to identify details of failure modes as well as how safety and security objectives are met both quantitatively and qualitatively. The equivalency of FFTs and the UML notation has been suggested (Bitsch, 2002; Hawkins et al., 2003). However, additional study and formalization of Use–Misuse Case and FFT equivalency language as well as automation of the translation process is required to fully exploit the potential advantages of this technique. Formalization of causal factors affecting safety and security, and their integration, is a subject of our ongoing research.

References

Policy and Economics Department, Association of American Railroads (AAR), 2007. Railroad Facts, 2007 ed. Association of American Railroads, Washington, DC.

Alexander, I., 2002. Initial industrial experience of misuse cases in trade-off analysis. In: Proceedings of 10th IEEE Joint International Requirements Engineering Conference (RE02), Essen, Germany, September 2002.

American Public Transportation Association (APTA), 2007. 2007 Public Transportation Fact Book. American Public Transportation Association, Washington, DC.

Bitsch, F., 2002. Requirements on methods and techniques in perspective to approval process for railway systems. In: Proceedings of the Second International Workshop on Integration of Specification Techniques for Applications in Engineering – Satellite Event of ETAPS 2002.

Braband, J., 1997. Safety and security requirements for an advanced train control system. In: Daniel, P. (Ed.), Computer Safety, Reliability, and Security (SAFECOMP 1997 York, UK). Springer, London.

Brabrand, J., Renpenning, F., 2001. Hazard and risk analysis for a low cost train control system. In: Proceedings of the 19th International System Safety Conference, Huntsville, Alabama, System Safety Society, Unionville, VA.

Bureau of Transportation Statistics (BTS), 2003. National Transportation Atlas Databases (2003) Federal Railroad Administration (FRA) National Rail Network 1:100,000 (line) 2003 ed. US Department of Transportation, Washington, DC.

Bureau of Transportation Statistics (BTS), 2008. White House Economic Statistics Briefing Room-Transportation: Amtrak Ridership. US Department of Transportation, Washington, DC.

Chabanon, D.K., 2005. How field-testing of a CBTC system fit into the safety case? NYCT Canarsie Line Case Study. In: Proceedings of the 2005 Rail Transit Conference, Pittsburg, PA, June 5–8, 2008. American Public Transportation Association, Washington, DC.

Evans, A., Verlander, N., 1996. Estimating the consequences of accidents: the case of automatic train protection in Britain. Accident Analysis and Prevention 28(2).

Federal Railroad Administration (FRA), 1999a. Railroad Communications and Train Control. Report to Congress, US Department of Transportation, Washington, DC.

Federal Railroad Administration (FRA), 1999b. Report of the Railroad Safety Advisory Committee to the Federal Railroad Administrator, Implementation of Positive Train Control System. US Department of Transportation, Washington, DC.

Federal Railroad Administration (FRA), 2007. Trespass on Railroad Right of Way. Research Results June 7–19, 2007, US Department of Transportation, Washington, DC.

Federal Railroad Administration (FRA), 2008. Rail-Trespasser Fatalities: Developing Demographic Profiles, March 2008. US Department of Transportation, Washington, DC.

Gheorghe, A., Birchmeier, J., Vamanu, D., Papazoglou, I., Kroger, W., 2005. Comprehensive risk assessment for rail transportation of dangerous goods: a validated platform for decision support. Reliability Engineering and System Safety 88(3).

Government Printing Office (GPO), 2008. PL110-432, Federal Railroad Safety Improvement Act of 2008. Congressional Record Senate, Washington, DC.

Government Printing Office (GPO), 2009a. Title 49 US Code of Federal Regulations Part 236 Subparts A through G. Washington, DC.

Government Printing Office (GPO), 2009b. Title 49 US Code of Federal Regulations Part 236 Subpart H. Washington, DC.

Government Printing Office (GPO), 2010. Title 49 US Code of Federal Regulations Part 236 Subpart H. Washington, DC.

Hartong, M., Goel, R., Wijesekera, D., 2006a. Communications based positive train control systems architecture in the USA. In: Proceedings of the 63rd IEEE International Vehicle Technology Conference, Melbourne, Australia, May 7–10, 2006.

Hartong, M., Goel, R., Wijesekera, D., 2006b. Mapping misuse cases to functional fault trees for positive train control security. In: Proceedings of the Ninth International Conference on Applications of Advanced Technology in Transportation Engineering, Chicago, IL, August 13–16, 2006.

Hawkins, R., Toyn, I., Bate, I., 2003. An approach to designing safety critical systems using the unified modeling language. In: Critical Systems Development with UML – Proceedings of the UML'03 Workshop, San Francisco, CA, October 2003.

US House of Representatives, Transportation and Infrastructure Subcommittee on Railroads (HR), 2003. Hearing on National Rail Infrastructure Financing Proposals. Washington, DC.

Jackson, K., 2005. Communications based (Positive) Train Control – consistent safety assessment for diverse technical approaches. In: Proceedings of the 2005 Rail Transit Conference, Pittsburg, PA, June 5–8, 2008. American Public transportation Association, Washington, DC.

Jo, H., Hwang, J., 2007. Investigation of risk analysis methods for safety assurance in the train control system. In: Proceedings of the International Conference on Electrical Machines and Systems, Seoul, Korea, October 8–11, 2007.

Jo, H., Hwang, J., Kim, Y., 2007. Risk assessment method for guaranteeing safety in the train control system. In: Proceedings of the International Conference on Urban Transport and the Environment, Urban Transport and the Environment in the 21st Century, Southampton, WIT.

Katsumata, P., Ho, V., Walecki, K., 2000. Lessons learned from a fault tree analysis of an automatic train protection system probabilistic safety assessment and management. In: Kondo, S., Furuta, K. (Eds.), PSAM 5, Osaka, Japan, November 27–December 1, 2000. Universal Academy Press, Tokyo.

Lawson, H., 2007. Provisioning of safe train control in Nordic countries. In: History of Nordic Computing 2, Second IFIP WG9.7 Conference, Turku, Finland, August 21–23, 2007, Advances in Information and Communications Technology, vol. 303. Springer.

Melago, C., 2008. Catastrophic CA. Train Wreck Caused When Metrolink Engineer Failed To Stop, Say Rail Officials. Daily News (New York City), September 13, 2008.

Mokkapatia, C., 2004. A practical risk and safety assessment for safety critical systems. In: Proceedings of the 2004 American Railway Engineering and Maintenance of Way Association Conference, Nashville, TN, May 17–18, 2004. American Railway Engineering and Maintenance of Way Association, Lanham, MD.

Monfaclone, M., Kaufman, L., Giras, T., 2001. Safety assessment of a direct traffic control (DTC) train control system using the axiomatic safety-critical assessment process (ASCAP). In: Proceedings of the Annual Reliability and Maintainability Symposium, Philadelphia, PA, January 22–25, 2001. IEEE.

Noffsinger, J., Giras, T., Johnson, B., 1999. A Safety Critical Methodology for Signaling and Train Control Systems. American Railway Engineering and Maintenance of Way Association. Communications and Signals Functional Group. American Railway Engineering and Maintenance of Way Association, Landover, MD.

National Transportation Safety Board (NTSB), 2005. Collision of Norfolk Southern Freight Train 192 with Standing Norfolk Southern Local Train P22 with Subsequent Hazardous Material Release at Graniteville, SC, January 6, 2005. NTSB #RAR-05/04, November 2005. National Transportation Safety Board, Washington, DC.

National Transportation Safety Board (NTSB), 2006. Collision of Union Pacific Railroad Train MHOTU-25 with BNSF Railway Company Train MEAP-TUL-126-D with Subsequent Derailment and Hazardous Materials Release, Macadona, TX, June 28, 2004. NTSB #RAR-06/03, July 2006. National Transportation Safety Board, Washington, DC.

National Transportation Safety Board (NTSB), 2007. Most Wanted List-Transportation Safety Improvements 2008. National Transportation Safety Board, Washington, DC.

Object Management Group, 2005. UML Superstructure Specification, v2.0 (formal/05-07-04), August 2005. OMG.

Opdahl, A., Sindre, G., 2001. Capturing security requirements through misuse cases. In: Proceedings, NorskInformatikkonferanse 2001, Universiteteti Tromsø, Norway, November 2001.

Surface Transportation Board, Office of Economics, Environmental Analysis and Administration (STB), 2003. Statistics of Class I Freight Railroads in the United States, 2003. Surface Transportation Board, Washington, DC.

Vesely, W., Roberts, H., Goldberg, F., Hassl, D., 1981. NUREG-0492 Fault Tree Handbook. US Nuclear Regulatory Commission, Washington, DC.

Yang, X., Xu, M., Cheng, Y., 2010. Risk analysis for the modification in automatic train control systems. In: Proceedings of the 2010 International Symposium on Computer Communication Control and Automation (3CA), Tainan, China, May 5–7, 2010.

Zhao, H., Xu, T., Tang, T., 2009. Towards modeling and evaluation of availability of communications based train control (CBTC) system. In: Proceedings of the 2009 IEEE International Conference on Communications Technology and Applications Communications Technology (ICCTA), Beijing, China, October 16–18, 2009.